Concerning the Cyclic Subgroups of the Simple Group G of all Linear Fractional Substitutions of Determinant Unity in Two Non-Homogeneous Variables with Coefficients in an Arbitrary Galois Field.[*]

By Leonard Eugene Dickson.

1. This paper leads to a generalization to the $GF[p^n]$ of certain results due to Professor Burnside[†] upon groups of linear substitutions in the $GF[p]$, i. e., the field of integers taken modulo p, a prime. Numerous variations from his method of treatment have been introduced in the present paper, partly to avoid the separate treatment of the two cases $d=1$ and $d=3$, and to enable us to catch in the exceptional cases $p=2$ and $p=3$, and partly to minimize the calculations and, on the other hand, to amplify certain proofs left to the reader. Professor Burnside's results for the case $p\equiv 1$ (mod. 3) are incorrect in two places. The factor 2 should be deleted from $\frac{N}{2(p-1)^2}$ on p. 103 and p. 104 of his paper; in fact, the statements made on p. 103, lines 15–23, are correct, but do not lead to the conclusion stated. A more subtle error was made on p. 102, lines 1–6. There exist three (and not just one) conjugate sets of substitutions of the canonical form there considered. This is made evident at the end of §4 below.

It has been possible to make the present treatment very brief and yet complete as to details, by making continual use of the general results of the paper on the "Canonical Form of a Linear Homogeneous Substitution in a Galois

[*] Presented in abstract at the meeting of December 28–29, 1899, of the Chicago Section of the American Mathematical Society.

[†] "On a Class of Groups Defined by Congruences," Proc. Lond. Math. Soc., vol. 26, pp. 58–106.

Field" (Amer. Jour. of Math., vol. XXII, pp. 121–137). We refer to this paper as "the earlier paper."

The distribution into conjugate sets of the substitutions of G is given by the formulæ (6), (7), (8), (9), (10), (11) and (12), the identical substitution forming another set.

From the results of this paper in the special case $p^n = 2^2$, we derive (§13) an immediate proof of the non-isomorphism of the alternating group on eight letters and our group G for $p^n = 2^2$, each being a simple group of order 20160. This result was first established by Miss Schottenfels under the direction of Professor Moore.*

2. The group G of all substitutions of determinant $|\alpha_{ij}| = 1$,

$$\mathrm{S}: \quad x' = \frac{\alpha_{11}x + \alpha_{12}y + \alpha_{13}}{\alpha_{31}x + \alpha_{32}y + \alpha_{33}}, \quad y' = \frac{\alpha_{21}x + \alpha_{22}y + \alpha_{23}}{\alpha_{31}x + \alpha_{32}y + \alpha_{33}},$$

in which the coefficients α_{ij} belong to the $GF[p^n]$, is a simple group of order†

$$N \equiv \frac{1}{d}(p^{3n} - 1)(p^{2n} - 1)p^{3n},$$

where d is the greatest common divisor of 3 and $p^n - 1$, so that

$$d = 1, \text{ if } p^n = 3^n \text{ or } 3l - 1; \quad d = 3, \text{ if } p^n = 3l + 1.$$

The equation $\tau^3 = 1$ has in the $GF[p^n]$ a single root $\tau = 1$, if $d = 1$, but has three roots $\theta, \theta^2, \theta^3 \equiv 1$, if $d = 3$. Hence, there are exactly d homogeneous substitutions of determinant unity

$$\xi_i' = \theta^r(\alpha_{i1}\xi_1 + \alpha_{i2}\xi_2 + \alpha_{i3}\xi_3) \qquad (i = 1, 2, 3)$$

which, when taken fractionally, lead to the same non-homogeneous substitution S of determinant unity. The homogeneous and non-homogeneous groups are, therefore, simply isomorphic if $d = 1$. For $d = 3$, we may still work with the homogeneous group in place of G, provided we regard as identical the three substitutions

$$\Sigma, \quad \Theta\Sigma \equiv \Sigma\Theta, \quad \Theta^2\Sigma \equiv \Sigma\Theta^2,$$

where Θ is the homogeneous substitution multiplying each index by θ.

* Annals of Mathematics, 2d Ser., vol. I, pp. 147–152.

† Part II of the writer's Chicago dissertation, Annals of Mathematics, vol. XI, 1897, pp. 161–183. Also Burnside, "Theory of Groups," p. 340.

3. We can exhibit G as a permutation-group on $p^{2n}+p^n+1$ letters. Every linear function $A\xi_1+B\xi_2+C\xi_3$, in which A, B, C are marks not all zero of the $GF[p^n]$, can be put into one of the forms

$$\mu(\xi_3+\rho\xi_2+\sigma\xi_1), \quad \mu(\xi_2+\rho\xi_1), \quad \mu\xi_1,$$

where μ, ρ, σ are marks of the $GF[p^n]$ and $\mu \neq 0$. Combining into one system $\{A\xi_1+B\xi_2+C\xi_3\}$ the p^n-1 linear functions $\mu(A\xi_1+B\xi_2+C\xi_3)$, μ denoting in succession the p^n-1 marks $\neq 0$ of the field, we obtain $p^{2n}+p^n+1$ distinct systems,

$$\{\xi_3+\rho\xi_2+\sigma\xi_1\}, \quad \{\xi_2+\rho\xi_1\}, \quad \{\xi_1\}, \qquad [\rho, \sigma \text{ arbitrary marks}].$$

Any ternary homogeneous linear substitution replaces the functions $\mu(A\xi_1+B\xi_2+C\xi_3)$, comprising one system, by linear functions

$$\mu(A\xi_1'+B\xi_2'+C\xi_3') \equiv \mu(\alpha\xi_1+\beta\xi_2+\gamma\xi_3),$$

all belonging to a single system. Hence, it permutes the above $p^{2n}+p^n+1$ symbols amongst themselves. It follows that G is isomorphic with a permutation-group G' on these symbols. But a homogeneous substitution altering none of the symbols must have the form

$$\xi_1'=\alpha\xi_1, \quad \xi_2'=\alpha\xi_2, \quad \xi_3'=\alpha\xi_3.$$

If it have determinant unity, it corresponds in G to the identity. Hence, G is *simply* isomorphic with G'.

The permutation-group G' is doubly transitive. We need only prove that G' contains a permutation converting $\{\xi_1\}$, $\{\xi_2+\xi_1\}$ into respectively

$$\{A\xi_1+B\xi_2+C\xi_3\}, \quad \{A'\xi_1+B'\xi_2+C'\xi_3\},$$

the latter being any two distinct symbols, viz.:

$$A:B:C \neq A':B':C'.$$

For the corresponding homogeneous substitution, we may take

$$\xi_1'=A\xi_1+B\xi_2+C\xi_3, \quad \xi_2'=(A'-A)\xi_1+(B'-B)\xi_2+(C'-C)\xi_3,$$
$$\xi_3'=\alpha\xi_1+\beta\xi_2+\gamma\xi_3,$$

where α, β, γ are chosen in any manner such that the determinant of the substitution is unity, viz.:

$$\alpha \begin{vmatrix} B & C \\ B' & C' \end{vmatrix} + \beta \begin{vmatrix} C & A \\ C' & A' \end{vmatrix} + \gamma \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = 1 .$$

By hypothesis the determinants are not all zero, so that solutions α, β, γ in the $GF[p^n]$ certainly exist.

4. By application of the general theorem of §2 of the earlier paper, a ternary homogeneous substitution of determinant unity in the $GF[p^n]$ can be reduced by a linear transformation of indices to one of the following five types of canonical forms:*

$$x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \lambda^{p^{2n}} z \qquad [\lambda^{p^{2n}+p^n+1} = 1] \quad (1)$$

arising when the characteristic determinant

$$\Delta(\lambda) \equiv \lambda^3 - \alpha\lambda^2 + \beta\lambda - 1$$

is irreducible in the $GF[p^n]$, its (imaginary) roots being, therefore, λ, λ^{p^n}, $\lambda^{p^{2n}}$.

$$x' = \mu x, \quad y' = \mu^{p^n} y, \quad z' = \mu^{-(p^n+1)} z, \qquad (2)$$

arising when $\Delta(\lambda)$ has a quadratic irreducible factor with roots μ, μ^{p^n} and a linear factor, whose root must evidently be the reciprocal of $\mu \,.\, \mu^{p^n}$, and, therefore, belongs to the $GF[p^n]$.

For the remaining types, the roots of $\Delta(\lambda) = 0$ all belong to the $GF[p^n]$. In the case of multiple roots, there arises more than one type of canonical form

$$\begin{array}{llll} x' = \alpha x, & y' = \beta y, & z' = \gamma z, & [\alpha\beta\gamma = 1], \quad (3) \\ x' = \alpha x, & y' = \beta y, & z' = \beta(z + y), & [\alpha\beta^2 = 1], \quad (4) \\ x' = \alpha x, & y' = \alpha(y + x), & z' = \alpha(z + y), & [\alpha^3 = 1]. \quad (5) \end{array}$$

In the last form we may set $\alpha = 1$ when applying our results to the group G.

* An interchange of the indices does not give rise to a new type, e. g.,

$$x' = \alpha x, \quad y' = \alpha(y + x), \quad z' = \beta z, \qquad [\alpha\beta^2 = 1].$$

Indeed, we can always make a new transformation of indices of determinant unity which interchanges any two indices and at the same time changes the signs of all three indices.

It will be convenient to treat the type (4) in two cases, according as $\alpha = \beta$ or $\alpha \neq \beta$, the order of (4) differing in the two cases.

If two substitutions S and T belong to the $GF[p^n]$ and have the same canonical form, there exists (by §8 of the earlier paper) a substitution W belonging to the field such that $T = W^{-1}SW$. It remains to consider whether or not there exists in the field a substitution W_1 of determinant unity which transforms S into T. Let w be the determinant of W.

For the canonical forms (1), (2), (3) and (4), it will be shown that each canonical form can be transformed into itself (retaining the same properties concerning the conjugacy of its indices) by a substitution V of determinant equal to an arbitrary mark $\neq 0$ of the field, in particular, one of determinant w^{-1}. Expressing it in the initial indices, we obtain a substitution V_1 belonging to the field, and of determinant w^{-1}, and, finally, transforming S into itself. Hence, the product $V_1 W$ will be the required substitution of determinant $w^{-1}.w = 1$, which belongs to the field and transforms S into T. Hence, will two substitutions in the $GF[p^n]$, which have the same canonical form (1), (2), (3) or (4), be conjugate within the group of substitutions in the field and having determinant unity.

For the type (1), we may take as V the substitution

$$x' = \sigma^r x, \quad y' = \sigma^{rp^n} y, \quad z' = \sigma^{rp^{2n}} z,$$

where σ is a primitive root in the $GF[p^{3n}]$, so that

$$\rho \equiv \sigma^{1+p^n+p^{2n}}$$

is a primitive root in the $GF[p^n]$. The determinant of V is, therefore, ρ^r, which, by proper choice of r, may be made equal to an arbitrary mark $\neq 0$ of the $GF[p^n]$.

For the types (2) and (3), we may take V to be

$$x' = x, \quad y' = y, \quad z' = \rho^r z.$$

For the type (4), we may take as V the substitution

$$x' = \rho^r x, \quad y' = y, \quad z' = z.$$

For the type (5), there arise two cases. If $d = 1$, so that 3 is prime to $p^n - 1$, every mark in the $GF[p^n]$ is a cube. Hence, we can determine r so that ρ^{3r} shall take an arbitrary value except zero in the field. Hence, we can take V to be

$$x' = \rho^r x, \quad y' = \rho^r y, \quad z' = \rho^r z.$$

But, for $d = 3$, only $(p^n - 1)/3$ of the marks $\neq 0$ are cubes,* their products by β and β^2 being not-cubes, if β be any particular not-cube. We can evidently determine V such that T is the transformed of S by a substitution $V_1 W$ belonging to the field and having as determinant 1, β or β^2. There remain three types

$$x' = x, \quad y' = y + x, \quad z' = z + y; \qquad (5_1)$$
$$x' = x, \quad y' = y + \beta x, \quad z' = z + y; \qquad (5_2)$$
$$x' = x, \quad y' = y + \beta^2 x, \quad z' = z + y; \qquad (5_3)$$

all conjugates by means of a substitution in the field, but of determinant $\neq 1$. In fact, the substitution

$$B: \quad \bar{x} = \beta x, \quad \bar{y} = y, \quad \bar{z} = z$$

transforms (5_2) into (5_1), while B^2 transforms (5_3) into (5_1). The most general substitution which transforms (5_1) into (5_2) is seen to be†

$$A: \quad x' = \frac{c}{\beta} x, \quad y' = cy + bx, \quad z' = cz + by + ax,$$

of determinant c^3/β, which cannot be unity. The most general substitution which transforms (5_2) into (5_3) is

$$A': \quad x' = \frac{c}{\beta} x, \quad y' = cy + \beta bx, \quad z' = cz + by + \beta ax,$$

gotten by transforming A by B^{-1}. But A' has determinant $c^3/\beta \neq 1$. Hence, for our group G, the types (5_1), (5_2), (5_3) are all distinct.

* Annals of Mathematics, vol. XI, 1897, p. 176.

† By §9 of the earlier paper, it is impossible to transform (5_1) into $\Theta(5_2)$. We can verify this result otherwise. If S be a general substitution replacing x by $ax + by + cz$, the products $(5_1)S$ and $\Theta S(5_2)$ will replace x by the same function only when

$$\theta c = c, \quad \theta b = b + c, \quad \theta a = a + b.$$

Since $\theta \neq 1$, $c = 0$, and hence $b = 0$ and, finally, $a = 0$. But this is impossible.

5. Type (1). The substitution of determinant unity

$$\begin{pmatrix} \alpha & -\beta & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

has the characteristic determinant

$$\Delta(\lambda) \equiv \lambda^3 - \alpha\lambda^2 + \beta\lambda - 1.$$

Hence, there exist homogeneous linear substitutions whose characteristic determinant has the middle coefficients α and β arbitrary marks in the $GF[p^n]$, and, therefore, one whose root λ is a primitive root of the equation

$$\lambda . \lambda^{p^n} . \lambda^{p^{2n}} = 1.$$

The order of the corresponding substitution (1) is the least integer m for which

$$\lambda^m = \lambda^{mp^n} = \lambda^{mp^{2u}},$$

i. e., for which $m(p^n - 1)$ is a multiple of $p^{2n} + p^n + 1$. But the greatest common divisor of $p^n - 1$ and $p^{2n} + p^n + 1$ is also that of $p^n - 1$ and 3, and, therefore, equals d. The order m is consequently $\frac{1}{d}(p^{2n} + p^n + 1)$.

Moreover, the roots of any irreducible cubic of the form $\Delta(\lambda) = 0$ are of the form λ^s, λ^{sp^n}, $\lambda^{sp^{2n}}$, so that the corresponding substitution is the s^{th} power of the substitution just considered. Hence, the orders of all substitutions having irreducible characteristic determinants are factors of $\frac{1}{d}(p^{2n} + p^n + 1)$.

Consider a substitution S of type (1) for which λ is a primitive root of

$$\lambda^{p^{2n} + p^n + 1} = 1. \qquad (a)$$

By §§5 and 9 of the earlier paper, the only substitutions of G which are commutative with S have the canonical form (simultaneously with the canonical form (1) of S):

$$x' = \sigma^r x, \quad y' = \sigma^{rp^n} y, \quad z' = \sigma^{rp^{2n}} z, \qquad (\sigma^{r(1+p^n+p^{2n})} = 1),$$

where σ is a primitive root of the $GF[p^{3n}]$. Hence, $r(1 + p^n + p^{2n})$ must be divisible by $p^{3n} - 1$, and, therefore, r divisible by $p^n - 1$. Setting $r = \rho(p^n - 1)$,

$$\sigma^r = (\sigma^{p^n - 1})^\rho = \lambda^{t\rho},$$

since σ^{p^n-1} is a primitive root of (a) and hence equal to some power t of λ. The only substitutions of G which are commutative with S are, therefore, the powers of S. It follows that S is one of a set of

$$s \equiv \frac{N}{1/d\,(p^{2n}+p^n+1)}$$

distinct conjugate substitutions, N being the order of G.

The only distinct powers of S which have the same characteristic determinant as S are evidently S, S^{p^n} and $S^{p^{2n}}$. To each set of three substitutions such as S^r, S^{rp^n}, $S^{rp^{2n}}$ contained in the cyclic group generated by S and all belonging to the same characteristic determinant, there corresponds a set of s distinct conjugate substitutions. Hence, there exist in G

$$\tfrac{1}{3}\left[\frac{1}{d}\,(p^{2n}+p^n+1)-1\right]$$

such sets of conjugate substitutions. It follows that G contains in all

$$\frac{dN}{3\,(p^{2n}+p^n+1)}\left[\frac{1}{d}\,(p^{2n}+p^n+1)-1\right] \tag{6}$$

substitutions not the identity whose orders are factors of $\frac{1}{d}\,(p^{2n}+p^n+1)$. Hence, there are $\frac{dN}{3\,(p^{2n}+p^n+1)}$ distinct cyclic subgroups of order $\frac{1}{d}\,(p^{2n}+p^n+1)$, all conjugate under G. Each must, therefore, be contained self-conjugately in a subgroup of G of order $\frac{3}{d}\,(p^{2n}+p^n+1)$.

6. Type (2). Since G contains substitutions in whose characteristic determinant $\Delta(\lambda) \equiv \lambda^3 - \alpha\lambda^2 + \beta\lambda - 1$, both α and β are arbitrary in the $GF[p^n]$, we can choose

$$\alpha \equiv \gamma + 1/\delta, \quad \beta \equiv \delta + \gamma/\delta,$$

so that

$$\Delta(\lambda) \equiv (\lambda - 1/\delta)(\lambda^2 - \gamma\lambda + \delta),$$

where γ and δ are arbitrary in the $GF[p^n]$. In particular, G contains a substitution T whose characteristic determinant has an irreducible quadratic factor which vanishes for a primitive root μ of the $GF[p^{2n}]$. The canonical form of T

is then (2). The order of T is, therefore, the least integer t for which

$$\mu^t = \mu^{tp^n} = \mu^{-t(p^n+1)},$$

i. e., for which both $t(p^n - 1)$ and $t(p^n + 2)$ are divisible by $p^{2n} - 1$. But $3t$ and $t(p^n - 1)$ are both divisible by $p^{2n} - 1$, for t a minimum, if and only if,

$$t = p^{2n} - 1, \text{ when } p^n = 3^n \text{ or } 3l - 1; \ t = \tfrac{1}{3}(p^{2n} - 1), \text{ when } p^n = 3l + 1.$$

Hence, the order of T is $\frac{1}{d}(p^{2n} - 1)$.

By §§5 and 9 of the earlier paper, the most general substitution of G, which is commutative with T, has the canonical form

$$x' = \mu^r x, \quad y' = \mu^{rp^n} y, \quad z' = \sigma z. \tag{c}$$

The determinant of (c) being unity,

$$\sigma = \mu^{-r(p^n+1)}.$$

Hence, (c) reduces to T^r. It follows that T is one of a set of $\frac{dN}{p^{2n} - 1}$ distinct conjugate substitutions. The only distinct powers of S which have the same multipliers as S are clearly S and S^{p^n}. Hence G contains $\frac{1}{2}\frac{dN}{p^{2n} - 1}$ distinct conjugate cyclic subgroups of order $\frac{1}{d}(p^{2n} - 1)$, each of which is thus contained self-conjugately in a subgroup of order $\frac{2}{d}(p^{2n} - 1)$.

The number of substitutions of G whose orders are factors of $\frac{1}{d}(p^{2n} - 1)$, without being at the same time factors* of $\frac{1}{d}(p^n - 1)$, is $\frac{1}{2}\frac{Np^n}{p^n + 1}$. In fact, such substitutions form

$$\frac{1}{2d}[(p^{2n} - 1) - (p^n - 1)] \equiv \frac{1}{2d}(p^n - 1)p^n$$

different sets, those in each set having the same characteristic determinant. It was

*If $d = 3$, the order is not a factor of $p^n - 1$, since the latter does not divide $\frac{1}{3}(p^{2n} - 1)$ when $p^n = 3l + 1$.

shown above that each such set contains $\frac{dN}{p^{2n}-1}$ distinct conjugate substitutions. The product gives the total number of such substitutions in G:

$$\frac{1}{2d}(p^n-1)p^n \cdot \frac{dN}{p^{2n}-1} \equiv \tfrac{1}{2}\frac{Np^n}{p^n+1}. \tag{7}$$

7. Type (4), for $\alpha \neq \beta$. Changing the notation, we consider the substitution P,

$$x' = \alpha(x+y), \quad y' = \alpha y, \quad z' = \alpha^{-2}z, \qquad (\alpha^3 \neq 1)$$

where α is a primitive root in the $GF[p^n]$. It generates a cyclic group of order $\frac{1}{d}p(p^n-1)$. If $p^n = 2$ or 2^2, we have $\alpha^2 = 1$, so that these two cases are here excluded; the reasoning below would, in fact, fail, since the order P is p for these two cases.

Considered as an operation of the isomorphic permutation-group, P belongs to a subgroup of G which leaves fixed the symbols $\{y\}$ and $\{z\}$. The general substitution possessing this property has the form

$$R: \quad x' = \alpha x + \alpha' y + \alpha'' z, \quad y' = \beta y, \quad z' = \gamma z. \qquad [\alpha\beta\gamma = 1].$$

In order that R shall have the order $\frac{1}{d}p(p^n-1)$, it is necessary and sufficient that α be a primitive root in the $GF[p^n]$, and that either

$$\text{(i).}\ \alpha' \neq 0, \quad \alpha = \beta \neq \gamma; \text{ or (ii).}\ \alpha'' \neq 0, \quad \alpha = \gamma \neq \beta.$$

Indeed, if both β and γ differ from α, we may, by introducing in place of x, the new index

$$X \equiv x + \frac{\alpha'}{\alpha-\beta}y + \frac{\alpha''}{\alpha-\gamma}z,$$

give R the form

$$X' \equiv \alpha X, \quad y' = \beta y, \quad z' = \gamma z,$$

whose $(p^n-1)^{\text{st}}$ power is unity. If, therefore, $\alpha \neq \beta$, we may take $\alpha = \gamma$. Then $\alpha'' \neq 0$; for, if $\alpha'' = 0$, R multiplies $x + \frac{\alpha'}{\alpha-\beta}y$ by α, so that R would have as order a factor of (p^n-1). Similarly, if $\alpha \neq \gamma$, then must $\alpha = \beta$, $\alpha' \neq 0$.

Finally, if $\alpha=\beta=\gamma$, each may be taken equal to unity. Then, by induction,

$$R^r:\quad x'=x+r\alpha' y+r\alpha'' z,\quad y'=y,\quad z'=z,$$

so that R is of period p. Hence, either (i) or (ii) are necessary conditions.

Consider the case when the relations (i) are satisfied. Setting

$$X\equiv x+\frac{\alpha'' z}{\beta-\gamma},\quad Y\equiv\frac{\alpha'}{\alpha}y,$$

R takes the form

$$X'=\alpha\,(X+Y),\quad Y'=\alpha Y,\quad z'=\alpha^{-2}z.$$

This substitution is of period $\frac{1}{d}\,p\,(p^n-1)$ if, and only if, α be a primitive root in the $GF[p^n]$.

Interchanging y with z, the proof follows for case (ii).

With the aid of the theorem just proven, we proceed to determine the number and conjugacy of the cyclic groups of order $\frac{1}{d}\;p\,(p^n-1)$, which leave the symbols $\{y\}$ and $\{z\}$ fixed. Consider first the case (i),

$$\alpha'\neq 0,\quad \alpha=\beta,\quad \gamma=\alpha^{-2}\neq\alpha,\qquad \alpha=\text{primitive root in the } GF[p^n]\,;$$
$$R:\quad x'=\alpha x+\alpha' y+\alpha'' z,\quad y'=\alpha y,\quad z'=\alpha^{-2}z.$$

By simple induction we verify that R^t has the form

$$x'=\alpha^t x+t\alpha'\alpha^{t-1}y+\alpha''\,\alpha^{t-1}\left(\frac{\alpha^{-3t}-1}{\alpha^{-3}-1}\right)z,\quad y'=\alpha^t y,\quad z'=\alpha^{-2t}z.$$

In order that ΘR^t shall be identical with

$$x'=\alpha x+\rho' y+\rho'' z,\quad y'=\alpha y,\quad z'=\alpha^{-2}z,$$

it is necessary and sufficient that

$$\theta\alpha^{t-1}=1,\quad t\alpha'=\rho',\quad \alpha''=\rho''.$$

It follows that the set of $p^n.\frac{p^n-1}{p-1}$ distinct substitutions

$$x'=\alpha x+My+\alpha'' z,\quad y'=\alpha y,\quad z'=\alpha^{-2}z, \tag{d}$$

where α is a fixed mark $\neq 0$, α'' an arbitrary mark, and M any one of the $\frac{p^n-1}{p-1}$ distinct marks M_1, M_2, ... such that no two have as their ratio an *integral* mark,* has the property that no power of one of the substitutions (d) equals another substitution of the set. We, therefore, obtain $p^n(p^n-1)/(p-1)$ distinct cyclic subgroups of order $\frac{1}{d}p(p^n-1)$.

Furthermore, every substitution V of the subgroup leaving $\{y\}$ and $\{z\}$ fixed, and having $\alpha=\beta$, and lastly of order a factor of $\frac{1}{d}p(p^n-1)$ without being a factor of p or (p^n-1), is contained in one of these cyclic subgroups. In proof, we observe that, by the argument used at the beginning of the paragraph, we may set

$$V:\quad x'=\alpha^s x+\alpha' y+\alpha'' z,\quad y'=\alpha^s y,\quad z'=\alpha^{-2s}z,\qquad (\alpha'\neq 0,\ \alpha^{3s}\neq 1).$$

Let M_i be such a mark that its ratio to α'/α^{s-1} is an integral mark. Then the power $s+k(p^n-1)$ of the substitution of the form (d) above

$$x'=\alpha x+M_i y+Az,\quad y'=\alpha y,\quad z'=\alpha^{-2}z,$$

is

$$x'=\alpha^s x+[s+k(p^n-1)]\,\alpha^{s-1}M_i y+A\alpha^{s-1}\left(\frac{\alpha^{-3s}-1}{\alpha^{-3}-1}\right)z,\quad y'=\alpha^s y,\quad z'=\alpha^{-2s}z.$$

By choice of k, we can make

$$[s+k(p^n-1)]\,\alpha^{s-1}M_i=\alpha',$$

and, by choice of A, we can make the coefficient of z in x' equal to α''. It follows that there are $p^n(p^n-1)/(p-1)$ cyclic subgroups of order $\frac{1}{d}p(p^n-1)$ for which $\alpha=\beta$, and as many more for which $\alpha=\gamma$, each leaving the symbols $\{y\}$ and $\{z\}$ fixed, and together containing all substitutions of the last property having an order not p nor a factor of p^n-1.

These cyclic subgroups are all conjugate within G, and, indeed, within the subgroup which leaves $\{y\}$ and $\{z\}$ fixed or permutes them. In proof, we first observe that the cases for which $\alpha^{-2}=\alpha$, viz., $p^n=2$ and $p^n=4$, have been excluded. We verify that the substitution

$$x'=x+\frac{B-A}{\alpha^{-2}-\alpha}z,\qquad y'=y,\qquad z'=z$$

* The marks M_1, M_2, ... are evidently the multipliers in a rectangular array of the marks $\neq 0$ of the $GF[p^n]$, the first row being formed by the integral marks 1, 2, ..., $p-1$.

transforms the substitution

$$x' = \alpha x + My + Az \quad , \quad y' = \alpha y, \quad z' = \alpha^{-2} z$$

into

$$x' = \alpha x + My + Bz \quad , \quad y' = \alpha y, \quad z' = \alpha^{-2} z.$$

Further,

$$x' = \lambda\rho x \quad , \quad y' = \rho y, \quad z' = \lambda^{-1}\rho^{-2} z$$

transforms

$$x' = \alpha x + My + Az \quad , \quad y' = \alpha y, \quad z' = \alpha^{-2} z$$

into

$$x' = \alpha x + \lambda My + \lambda^2\rho^3 Az, \quad y' = \alpha y, \quad z' = \alpha^{-2} z.$$

Hence the cyclic subgroups given by $\alpha = \beta$ are all conjugate within the group, leaving $\{y\}$ and $\{z\}$ fixed.

The substitution

$$x' = x \quad , \quad y' = -z \quad , \quad z' = y$$

interchanges $\{y\}$ with $\{z\}$ and transforms

$$x' = \alpha x + My + Az, \quad y' = \alpha y \quad , \quad z' = \alpha^{-2} z$$

into

$$x' = \alpha x - Ay + Mz, \quad y' = \alpha^{-2} y, \quad z' = \alpha z.$$

Hence the set of cyclic groups given by $\alpha = \beta$ are conjugate to the set given by $\alpha = \gamma$ within the group, leaving fixed $\{y\}$ and $\{z\}$ or permuting them. The latter group, therefore, contains $2p^n(p^n - 1)/(p - 1)$ conjugate cyclic groups of order $\frac{1}{d}\, p\,(p^n - 1)$, and those substitutions of these groups whose orders are not divisors of p or $(p^n - 1)$ are all distinct. But the general permutation-group is doubly transitive, and hence contains

$$\tfrac{1}{2}(p^{2n} + p^n + 1)(p^{2n} + p^n)$$

conjugate subgroups, leaving fixed two symbols or permuting them. In all, we have

$$2p^n\left(\frac{p^n - 1}{p - 1}\right) \cdot \tfrac{1}{2}(p^{2n} + p^n + 1)(p^{2n} + p^n) \equiv \frac{dN}{p^n(p^n - 1)(p - 1)}$$

conjugate cyclic subgroups of order $\frac{1}{d}\, p\,(p^n - 1)$. Each is, therefore, contained self-conjugately in a subgroup of order $\frac{1}{d}\, p^n(p^n - 1)(p - 1)$.

Each cyclic subgroup contains $p+\frac{1}{d}(p^n-1)-1$ substitutions of order p or a divisor of $\frac{1}{d}(p^n-1)$, the latter giving all of its substitutions whose orders divide p^n-1. There remain $(p-1)\Big[\frac{1}{d}(p^n-1)-1\Big]$ substitutions. Hence, G contains

$$\frac{N(p^n-1-d)}{p^n(p^n-1)} \tag{8}$$

substitutions whose orders divide $\frac{1}{d}\,p\,(p^n-1)$ but not p or p^n-1. For the cases $p^n=2$ or 2^2 above excluded, formula (8) reduces to zero. The result is, therefore, true generally.

8. Type 4, when $\alpha=\beta$. We have to consider substitutions of order p of the canonical form

$$x'=x+z,\quad y'=y,\quad z'=z.$$

From the investigation at the beginning of §7, it follows that the only substitutions of period p which leave fixed the symbols $\{y\}$ and $\{z\}$ have the form

$$x'=x+\alpha y+\beta z,\quad y'=y,\quad z'=z, \tag{e}$$

(α and β not both zero.)

There are $p^{2n}-1$ distinct substitutions of this form. They are all conjugate within G, being reducible to the above canonical form. In fact, if $\beta \neq 0$, we transform (e) by

$$x'=x,\quad y'=y,\quad z'=z+\rho y$$

and get the substitution

$$x'=x+(\alpha-\beta\rho)\,y+\beta z,\quad y'=y,\quad z'=z.$$

By choice of ρ, we can make $\alpha-\beta\rho=0$. If $\beta=0$, we transform (e) by

$$x'=-x\quad,\ y'=z,\quad z'=y,$$

giving

$$x'=x-\alpha z,\quad y'=y,\quad z'=z.$$

In either case, we reach a substitution of the form (e), but having the coefficient $\alpha=0$, and, therefore, $\beta \neq 0$. Transforming it by

$$x'=x \quad, \quad y'=\beta^{-1}y, \quad z'=\beta z,$$

we get

$$x'=x+z, \quad y'=y \quad, \quad z'=z.$$

The $p^{2n}-1$ substitutions (e) determine $(p^{2n}-1)/(p-1)$ conjugate cyclic subgroups of order p and contained in the subgroup, leaving fixed the symbols $\{y\}$ and $\{z\}$, and hence also $\{y+\rho z\}$, ρ being an arbitrary mark in the $GF[p^n]$. Each such group, therefore, leaves fixed p^n+1 (and no more) symbols. But the $p^{2n}+p^n+1$ symbols furnish

$$\frac{\frac{1}{2}(p^{2n}+p^n+1)(p^{2n}+p^n)}{\frac{1}{2}(p^n+1)p^n} \equiv p^{2n}+p^n+1$$

such sets of symbols. Hence, G contains

$$(p^{2n}+p^n+1)\frac{(p^{2n}-1)}{(p-1)} \equiv \frac{dN}{p^{3n}(p^n-1)(p-1)}$$

such conjugate cyclic subgroups, all of whose substitutions are conjugate under G. Each such subgroup is, therefore, contained self-conjugately within a subgroup of order $\frac{1}{d}p^{3n}(p^n-1)(p-1)$. The total number of distinct substitutions of G of order p of the type considered has thus been shown to be

$$\frac{dN}{p^{3n}(p^n-1)}. \tag{9}$$

9. Type (5_1). If $p>2$, the substitution

$$W_1: \quad x'=x+y \quad y'=y+z, \quad z'=z,$$

is of order p. The most general substitution transforming W_1 into itself has the form

$$x'=ax+by+cz, \quad y'=ay+bz, \quad z'=az. \tag{f}$$

If it have determinant unity, $a = 1$, θ or θ^2. Hence, there are dp^{2n} such substitutions. The following substitution of determinant unity

$$x' = tx, \quad y' = y - \frac{t-1}{2t}z, \quad z' = \frac{1}{t}z$$

will transform W_1 into W_1^t, viz.:

$$W_1^t: \quad x' = x + ty + \tfrac{1}{2}t(t-1)z, \quad y' = y + tz, \quad z' = z.$$

Taking $t = 1, 2, \ldots, p-1$, we get $dp^{2n}(p-1)$ distinct homogeneous substitutions of determinant unity which transform into itself the cyclic group generated by W_1. There correspond $p^{2n}(p-1)$ distinct substitutions in G. The cyclic group $\{W_1\}$ is, therefore, one of $\frac{N}{p^{2n}(p-1)}$ distinct conjugate subgroups of G. Hence, G contains N/p^{2n} distinct conjugate substitutions of the type (5_1).

Since (5_2) and (5_3) are conjugate to (5_1) within the general linear homogeneous group, the number of substitutions of G conjugate within G to (5_1) equals the number conjugate to (5_2) or to (5_3). Hence, there are in G together

$$3N/p^{2n} \qquad (10)_{p>2}$$

distinct substitutions of the types (5_1), (5_2) and (5_3), forming three distinct sets of conjugate subgroups.

10. Types (5_1), (5_2) and (5_3) for $p = 2$. The order of the canonical types,

$$W_i: \quad x' = x + y, \quad y' = y + \beta^i z, \quad z' = z \qquad (i = 0, 1, 2)$$

is now 4. Indeed, we have

$$\begin{aligned} W_i^2: &\quad x' = x + \beta^i z, & y' &= y, & z' &= z; \\ W_i^3: &\quad x' = x + y + \beta^i z, & y' &= y + \beta^i z, & z' &= z. \end{aligned}$$

Since W_i leaves fixed but one symbol $\{z\}$, while W_i^2 leaves fixed the $2^n + 1$ symbols $\{z\}$, $\{y + \lambda z\}$ (λ = arbitrary mark of the $GF[2^n]$), the two substitutions are not conjugate under G. But W_i is transformed into W_i^3 by the substitution

$$x' = x + y, \quad y' = y, \quad z' = z.$$

As in §9, the most general substitution transforming W_i into itself is

$$x' = ax + by + cz, \quad y' = ay + b\beta^i z, \quad z' = az.$$

Its determinant must be unity, whence $a^3 = 1$. It follows that G contains just 2^{2^n} distinct substitutions which transform W_i into itself and, therefore, as many more which transform W_i into W_i^3. The cyclic group of order 4 generated by W_i is, consequently, one of $N/2^{2n+1}$ conjugate subgroups of G. Just two of the substitutions of every such subgroup are of type W_i, the remaining one,* $\neq I$, being of type (4) with $\alpha = \beta$. Hence, G contains

$$\frac{3N}{2^{2n}} \qquad (10)_{p=2}$$

distinct substitutions of the types (5_1), (5_2), (5_3) for $p = 2$, all distinct from those enumerated in §8. As in the case $p > 2$, they fall into three distinct sets of conjugate substitutions under G.

11. Type (3). The substitutions of the canonical form

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z \qquad [\alpha\beta\gamma = 1] \qquad (3)$$

are of order a divisor of $p^n—1$. Of the $(p^n— 1)^2$ sets of solutions in the $GF[p^n]$ of $\alpha\beta\gamma = 1$, d sets have $\alpha = \beta = \gamma$, and hence each equal to θ^r $(r = 0$, 1 or 2). If α be any mark different from 0, 1, θ, θ^2, and if $\beta = \alpha$, then $\gamma = \alpha^{-2} \neq \alpha$. Hence, there are $3\,(p^n — d — 1)$ sets of solutions, in which two, and only two, of the quantities α, β, γ are equal. There remain

$$(p^n — 1)^2 — 3\,(p^n — d — 1) — d \equiv p^{2n} — 5p^n + 4 + 2d$$

sets of solutions in which α, β, γ are all distinct. Dividing this number by 6 to allow for permutations, we obtain the number of distinct sets of unequal multipliers of ternary homogeneous substitutions (3).

If, for $d = 3$, α, β, γ do not form a permutation of 1, θ, θ^2, the three sets

$$\alpha, \beta, \gamma\,; \quad \theta\alpha, \theta\beta, \theta\gamma\,; \quad \theta^2\alpha, \theta^2\beta, \theta^2\gamma,$$

* W_1^2 and W_2^2 are readily transformed into W_0^2. For example, the substitution

$$x' = x, \quad y' = \beta^{-1}y, \quad z' = \beta z$$

of determinant unity, transforms W_1^2 into W_0^2.

are not equivalent sets of multipliers in the homogeneous group, but are equivalent in the non-homogeneous group G. The number of sets of unequal multipliers in G is, therefore,

$$1+\tfrac{1}{3}\left(\frac{p^{2n}-5p^n+4+2d}{6}-1\right),\ \text{for } d=3\,;\quad \frac{p^{2n}-5p^n+4+2d}{6},\ \text{for } d=1\,.$$

By §5 of the earlier paper, the only homogeneous substitutions commutative with (3), for α, β, γ distinct, are the $(p^n-1)^2$ substitutions

$$T:\quad x'=ax,\quad y'=by,\quad z'=cz,\qquad (abc=1).$$

By §9 of the earlier paper, there exist substitutions transforming S, given by (3), into ΘS only when α, β, γ form a permutation of 1, θ, θ^2. In the latter case, S has one of the forms T, PT, P^2T, where P denotes the substitution

$$P:\quad x'=y,\quad y'=z,\quad z'=x.$$

In this case, there are $3\,(p^n-1)^2$ homogeneous substitutions commutative with (3), and, therefore, $(p^n-1)^2$ substitutions of G commutative with the substitutions corresponding to (3) in G. Hence,

$$x'=x,\quad y'=\theta y,\quad z'=\theta^2 z$$

is one of a set $\dfrac{N}{(p^n-1)^2}$ distinct conjugate substitutions under G.

For α, β, γ distinct and not a permutation of 1, θ, θ^2, each substitution (3) is one of a set of $\dfrac{N}{1/d\,(p^n-1)^2}$ conjugate substitutions under G. The total number of such substitutions is, therefore,

$$\frac{dN}{(p^n-1)^2}\cdot\tfrac{1}{3}\left(\frac{p^{2n}-5p^n+4+2d}{6}-1\right),\ \text{for } d=3\,;$$

$$\frac{N}{(p^n-1)^2}\left(\frac{p^{2n}-5p^n+4+2d}{6}\right),\ \text{for } d=1\,.$$

Combining our results, the total number of substitutions of G of canonical form (3) in which α, β, γ are distinct, is for $d=1$ or 3:

$$\frac{N}{(p^n-1)^2}\cdot\frac{p^{2n}-5p^n+4+2d}{6}\,. \tag{11}$$

Consider next the $p^n - d - 1$ sets of multipliers α, β, γ, two of which are equal. There correspond to the substitutions (3) $1/d\,(p^n - d - 1)$ substitutions of G, no two of which are conjugate, having different sets of multipliers. The substitution

$$A: \quad x' = \alpha x, \quad y' = \alpha y, \quad z' = \gamma z \qquad [\alpha^2\gamma = 1,\ \gamma \neq \alpha]$$

cannot, by §9 of the earlier paper, be transformed into ΘA. The most general substitution transforming A into itself is, by §5 of the earlier paper,

$$x' = ax + by, \quad y' = a'x + b'y, z' = c''z.$$

The number of such substitutions of determinant unity is

$$(p^{2n} - 1)(p^{2n} - p^n).$$

Hence, the total number of substitutions of G having the canonical form A is

$$\frac{1}{d}\,(p^n - d - 1)\,.\,\frac{N}{1/d(p^{2n}-1)(p^{2n}-p^n)} \equiv \frac{N(p^n - d - 1)}{(p^{2n} - 1)(p^{2n} - p^n)}\,. \qquad (12)$$

12. As a check upon the accuracy of our enumeration of the substitutions of G, we may verify that the numbers given by the formulæ (6), (7), (8), (9), (10), (11) and (12), together with unity (to count the identical substitution), give as total sum the number N.

13. In determining the cyclic groups generated by the substitutions of type (3), we consider in turn the cases $d = 1$ and $d = 3$. If α be a primitive root of the $GF\,[p^n]$, any substitution C of the form (3) may be written

$$C: \quad x' = \alpha^r x, \quad y' = \alpha^s y, \quad z' = \alpha^{-r-s} z,$$

where r and s are integers chosen from the series 0, 1, 2, ... , $p^n - 2$. Then, for $d = 1$, C is of period $p^n - 1$ if, and only if, the greatest common divisor of r, s, and $p^n - 1$ is unity, or, symbolically, $[r, s, p^n - 1] = 1$. The number of sets of integers r, s satisfying this condition is (Jordan, "Traité," p. 96)

$$F(p^n - 1) \equiv \phi(p^n - 1)\,\psi(p^n - 1) \equiv (p^n - 1)^2\left(1 - \frac{1}{q_1^2}\right)\left(1 - \frac{1}{q_2^2}\right)\ \ldots\ ,$$

where q_1, q_2, ... are the distinct prime factors of $p^n - 1$. For $\phi\,(p^n - 1)$ values of r, the pairs r, r; r, $-2r$; $-2r$, r are included in these sets, but lead to only $\phi\,(p^n - 1)$ sets of multipliers in C. The remaining $F - 3\phi\,(p^n - 1)$ sets r, s lead to $\frac{1}{6}\{F(p^n - 1) - 3\phi\,(p^n - 1)\}$ sets of unequal multipliers in C.

The substitutions (3) all lie in the cyclic groups generated by substitutions C of period $p^n - 1$. In certain of these cyclic groups, the $\phi(p^n - 1)$ substitutions of period $p^n - 1$ have in pairs the same set of multipliers; in others they have by threes the same set of multipliers.* If C have the multipliers α, α^m, α^{-1-m}, where $m^2 \equiv 1 \pmod{p^n - 1}$, then C^m has the same multipliers in a different order. But if $m^2 + m + 1 \equiv 0 \pmod{p^n - 1}$, then C, C^m, C^{-1-m} all have the same set of multipliers. The first congruence has $2^{\mu+\kappa}$ solutions m, where μ denotes the number of distinct odd prime factors of $p^n - 1$; while, if 2^k is the highest power of 2 contained in $p^n - 1$, $\varkappa = 0$ if $k = 0$ or 1, $\varkappa = 1$ if $k = 2$, $\varkappa = 2$ if $k \geqq 3$ (Dirichlet, "Zahlentheorie," §37). The second congruence $m^2 + m + 1 \equiv 0$ is seen† to have solutions for $d = 1$ only when $p^n = 2^n$, n odd, such that the prime factors (say γ distinct ones) are all of the form $6j + 1$. But if m be a solution, so is also $-1 - m$, giving but $2^{\gamma-1}$ sets of multipliers α, α^m, α^{-1-m}. The solutions $m > 1$ of $m^2 \equiv 1$ lead to $2^{\mu+\kappa} - 1$ distinct cyclic groups of order $p^n - 1$, such that the sets of multipliers of their substitutions of period $p^n - 1$ are the same in pairs, and containing in all $\frac{1}{2}\phi(p^n - 1)(2^{\mu+\kappa} - 1)$ distinct sets of multipliers of substitutions of period $p^n - 1$. The solutions of $m^2 + m + 1 \equiv 0$ lead to $2^{\gamma-1}$ distinct cyclic groups of order $p^n - 1$, containing $\frac{1}{3}\phi(p^n - 1)\, 2^{\gamma-1}$ distinct sets of multipliers of substitutions of period $p^n - 1$, those in each cyclic group having coincided in sets of three. Denote by $\rho\phi(p^n - 1)$ the combined number of sets of multipliers in these two classes of cyclic groups. In every other cyclic subgroup, the sets of multipliers of the substitutions of period $p^n - 1$ are found to be distinct. Hence, the substitutions (3) generate the following classes of non-conjugate cyclic groups of order $p^n - 1$:

(i). $2^{\mu+\kappa} - 1$ groups generated by substitutions with multipliers α, α^m, α^{-1-m} with $m^2 \equiv 1 \pmod{p^n - 1}$, $m > 1$.

(ii). $2^{\gamma-1}$ groups with similar generators having $m^2 + m + 1 \equiv 0 \pmod{p^n - 1}$.

(iii). One group generated by the substitution with multipliers α, α, α^{-2}.

(iv). $\frac{1}{6}\{\psi(p^n - 1) - 3\} - \rho$ groups generated by substitutions with unequal multipliers and not conjugate with any of their powers.

A cyclic group of class (i), (ii), (iii) or (iv) is transformed into itself by the following number of substitutions of G respectively:

$$2(p^n - 1)^2, \quad 3(p^n - 1)^2, \quad (p^{2n} - 1)(p^{2n} - p^n) \text{ or } (p^n - 1)^2.$$

* The statements of Burnside, l. c., middle of p. 77, are not exact.

† Using Dirichlet, §§35 and 37, and Gauss, Disq. Arith., Art. 120.

In fact, each is commutative with the $(p^n - 1)^2$ substitutions C; class (iv) with no other substitutions of G; class (i) also with CT, where T replaces x by y and y by $-x$; class (ii) also with $(xyz)\,C$ and $(xzy)\,C$; class (iii) with

$$x' = ax + by, \quad y' = cx + dy, \quad z' = ez.$$

14. For $d = 3$, set $p^n - 1 = 3t$. We may establish the theorem:*

If t be prime to 3, *every substitution* (3) *is some power of a substitution* (3) *of period $p^n - 1$; if t be divisible by* 3, *no cyclic group of order $p^n - 1$ generated by a substitution* (3) *contains one of the substitutions of period t*

$$x' = \alpha x, \quad y' = \alpha^{3l+1} y, \quad z' = \alpha^{-3l-2} z.$$

Except when $p^n - 1$ is divisible by 9, it, therefore, suffices to study the cyclic groups of order $p^n - 1$. The substitution C is of period $p^n - 1$, if, and only if, $[r, s, p^n - 1] = 1$ and $r - s$ be prime to 3. Denote by M the number of sets of multipliers giving distinct substitutions C of period $p^n - 1$ in the quotient-group G. We can readily prove that, if t be prime to 3, $M = \frac{1}{3} F(t)$; while, if t be divisible by 3 and we set $t \equiv T 3^\tau$, T being prime to 3, then $M = 3^{2\tau - 1} F(T)$.

Supposing first that t is prime to 3, we may establish the following complete list of non-conjugate cyclic groups of order $p^n - 1$ generated by the substitutions (3):

(a). $2^{\mu + \kappa - 1}$ groups generated by substitutions with multipliers α, α^m, α^{-1-m}, where $m^2 \equiv 1 \pmod{3t}$, $m \equiv -1 \pmod{3}$.

(b). $2^{\delta - 1}$ groups generated by similar substitutions with $m^2 + m + 1 \equiv 0 \pmod{3t}$, $m \equiv 1 \pmod{3}$, occurring only when $p^n = 2^n$, n even and prime to 3, such that $\frac{1}{3}(2^n - 1)$ has only prime factors (δ distinct ones) of the form $6j + 1$.

(c). $\dfrac{1}{\phi(3t)} \{ \frac{1}{3} F(t) - \frac{1}{2} \phi(3t)\, 2^{\mu - 1 + \kappa} - \frac{1}{3} \phi(3t)\, 2^{\delta - 1} \}$ groups generated by substitutions of period $p^n - 1$ not conjugate with any of their powers.

If t be divisible by 3, the only cyclic groups of order $p^n - 1$ are:

(a). $2^{\mu + \kappa - 1}$ groups generated by substitutions with the multipliers α, α^m, α^{-1-m}, where $m^2 \equiv 1 \pmod{3t}$, $m \equiv -1 \pmod{3}$.

(b). $\dfrac{1}{\phi(3t)} \{ 3^{2\tau - 1} F(T) - 2^{\mu + \kappa - 1} . \frac{1}{2} \phi(3t) \}$ groups generated by substitutions of period $p^n - 1$ not conjugate with any of their powers.

* The statements of Burnside, l. c., p. 102, are not complete.

15. For the case $p^n = 2^2$, we have a simple group G of order $N \equiv 20160$. Applying the above general results to this case, G contains

	960	conjugate cyclic groups of order	7	with	5760	substitutions period	7
	2016	" " "	5	"	8064	" "	5
Three sets of	630	" " "	4	"	3.1260	" "	4
	315	" " "	2	"	315	" "	2
	1120	" " "	3	"	2240	" "	3
					1	identity.	
					20160		

The substitutions of period 2 are all contained in the cyclic groups of order 4.

For comparison, we give a table of the types of substitutions in the alternating group on 8 letters:

Type.	Period.	Number in G.
(1234567)	7	5760
(123456)(78)	6	3360
(12345)	5	1344
(12345)(678)	15	2688
(1234)(56)	4	2520
(1234)(5678)	4	1260
(123)	3	112
(123)(456)	3	1120
(123)(45)(67)	6	1680
(12)(34)	2	210
(12)(34)(56)(78)	2	105
identity	1	1
		20160

The two groups differ in structure in many respects. They contain the same number of substitutions of period 7, the same number of period 4 and the same number of period 2.

NOTE.—Page 232, line 6: For § 13 read § 15.

UNIVERSITY OF TEXAS, *December* 12, 1899.